(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－202877

(43)公開日　平成７年(1995)８月４日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		9364－5L		
				Ｈ０４Ｌ　9/ 00　Ｚ	

審査請求　未請求　請求項の数２　ＦＤ　（全 5 頁）　最終頁に続く

(21)出願番号　特願平5－353626

(22)出願日　平成５年(1993)12月27日

(71)出願人　594038346
株式会社ソフィック
大阪市都島区都島南通２丁目１番２－417号

(71)出願人　594066763
株式会社ツヨカ
大阪府大阪市淀川区西中島３丁目21番13号

(72)発明者　津村　三百次
大阪市都島区都島南通２丁目１番１－805号

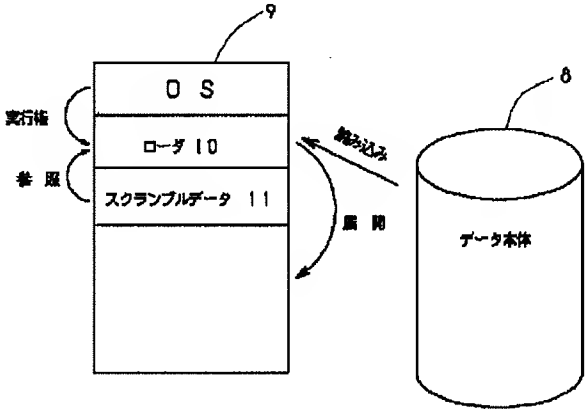
(74)代理人　弁理士　濱田　俊明　（外２名）

(54)【発明の名称】　データのスクランブル装置

(57)【要約】

【目的】　容易に復号されにくい暗号化のための装置を提供する。

【構成】　ホストコンピュータと複数の受信端末装置とからなり、このホストコンピュータから各受信端末装置に対して一方向通信によってスクランブルが施されたデータ本体をサイクリックで送信する一方、上記ホストコンピュータと各受信端末装置とは双方向通信網で接続され、各受信端末装置からの個別の要求に応じて上記ホストコンピュータから上記スクランブルを復号するスクランブルデータとデータ本体を実行するローダをダウンロードする。受信端末装置では、データ本体と、スクランブルデータと、ローダとを外部記憶装置にいったん格納し、主記憶装置の空領域に上記ローダとスクランブルデータを移行し、上記スクランブルデータを参照して上記ローダがデータ本体を展開する。



【特許請求の範囲】
【請求項１】ホストコンピュータと複数の受信端末装置とからなり、このホストコンピュータから各受信端末装置に対して一方向通信によってスクランブルが施されたデータ本体をサイクリックで送信する一方、上記ホストコンピュータと各受信端末装置とは双方向通信網で接続され、各受信端末装置からの個別の要求に応じて上記ホストコンピュータから上記スクランブルを復号するスクランブルデータとデータ本体を実行するローダをダウンロードすることを特徴としたデータのスクランブル装置。
【請求項２】受信端末装置では、データ本体と、スクランブルデータと、ローダとを外部記憶装置にいったん格納し、主記憶装置の空領域に上記ローダとスクランブルデータを移行し、上記スクランブルデータを参照して上記ローダがデータ本体を展開する請求項１記載のデータのスクランブル装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、無線あるいは有線通信において伝送されるデータにスクランブルを施すための新規な装置に関するものである。
【０００２】
【従来の技術】データ伝送技術は飛躍的に進歩し、現在ではパーソナルコンピュータ同士で電話回線や特定回線を利用して通信が行われている。また、無線によるデジタル通信技術も発達しており、ＰＣＭ通信なども盛んである。ところで伝送されるデータが無償の解放データである場合にはデータには特に加工を施すことなく、たとえばパケット通信のためのパケット番号や誤り訂正符号などを付記するだけで十分である。
【０００３】
【発明が解決しようとする課題】しかし、情報価値が高まっている現在、データの内容によっては秘密を要する頻度も非常に高くなっている。従って従来からデータ伝送では伝送の対称となるデータを送信する直前にエンコーダでスクランブルを施し、受信装置にはスクランブルを解除するためのデコーダを設けておき、取り決められたプロトコルに従って伝送を行うのが一般的である。
【０００４】ところが、スクランブルを施すためのエンコーダでは一定の手順に従ってデータを符号化するために、暗号化プログラムを持っているが、一度デコードされてしまうとデータが生の状態で蓄積されてしまう。従って、最初のデータ利用については利用料金を支払ったとしても、２度目からは料金なしで簡単に利用することができるようになり、実質的に無断使用の問題が発生する。
【０００５】本発明ではこれらの事実に鑑み、一度実行されても、再度は容易に復号されにくい暗号化のための装置を提供することを目的とする。
【０００６】
【課題を解決するための手段】本発明では上記目的を達成するために、ホストコンピュータと複数の受信端末装置とからなり、このホストコンピュータから各受信端末装置に対して一方向通信によってスクランブルが施されたデータ本体をサイクリックで送信する一方、上記ホストコンピュータと各受信端末装置とは双方向通信網で接続され、各受信端末装置からの個別の要求に応じて上記ホストコンピュータから上記スクランブルを復号するスクランブルデータとデータ本体を実行するローダをダウンロードするという手段を採用した。
【０００７】また、受信端末装置では、データ本体と、スクランブルデータと、ローダとを外部記憶装置にいったん格納し、主記憶装置の空領域に上記ローダとスクランブルデータを移行し、上記スクランブルデータを参照して上記ローダがデータ本体を展開するという手段を用いた。
【０００８】
【作用】ホストコンピュータから一方向通信でデータ本体を送信するのは、データ容量が大きいと考えられる部分を伝送効率が高い伝送モードに適用するためである。ホストコンピュータと各受信端末装置を双方向通信で接続する手段は、受信端末装置からの要求に応じたファイルの伝送を可能とするためである。データ本体にスクランブルを施して同報的に送信する手段は、データの無断利用を回避するものである。
【０００９】
【実施例】以下、本発明の一実施例を、添付した図面に従って説明する。先ず、データ伝送のためのシステムとしては図１あるいは図２のネットワークが採用される。図１は衛星通信および公衆回線網を用いたネットワークであり、１はデータ供給側のホストコンピュータ、２…２はそれぞれ受信端末装置、３は通信衛星、４はデジタル回線などの公衆回線網である。ホストコンピュータ１からは受信端末装置２に対して一方向通信で情報が伝送されると共に、公衆回線網４によって双方向通信が行われる。図２はＣＡＴＶネットワークを用いたものであり、ホストコンピュータ１と受信端末装置２…２とは光通信などを利用したＣＡＴＶネットワーク５で接続されている。本実施例で採用するＣＡＴＶネットワーク５は双方向通信を可能とするもので、６は上りライン、７は下りラインである。ただし、既存の一方向通信機能を有するＣＡＴＶネットワークを利用するときには、上りライン６に公衆回線網が代替することも自由である。
【００１０】次に、本発明で伝送の対象となるデータ構造としては、データ本体と、スクランブルデータと、ローダによって構成されている。そして、多数のデータ本体がホストコンピュータ１から通信衛星３、あるいはＣＡＴＶネットワーク５を介して受信端末装置２に対してサイクリックに送信され、スクランブルデータとローダ

は各受信端末の要求に応じて公衆回線網４を介して個別に送信される。あるいは、ＣＡＴＶネットワーク５の場合にはデータ本体とは別チャンネルで個別の識別符号を付加するなどの処理を施したうえで送信される。このようにデータを２種類の伝送経路に分割するのは、データ本体はデータ容量が膨大なものも存在するので、伝送効率が高い通信モードに適する一方、スクランブルデータやローダなどはデータ容量は小さいが、料金徴収との関係で要求先である受信端末装置を特定する必要があるからである。

【００１１】送信の対象となるデータ本体はスクランブルが施された状態のもので、スクランブルデータはスクランブルのパラメータや、スクランブルの一種としての圧縮辞書やパスワードなどによって構成されている。また、ここでいうデータ本体とは、実行ファイルを含んだデータを意味し、一定のコマンドによってデータ本体単独で起動することができるものをいう。ローダはデータ本体を起動するために用いられ、データ本体をスクランブルデータに基づいて復号しながら、受信端末に装備された主記憶装置の空メモリ領域やハードディスクなどの外部記憶装置に展開する。そして実行権を、復号されたデータ本体に移行する。このとき、スクランブルデータもローダと共に主記憶装置あるいは外部記憶装置に展開される。従って、主記憶装置にいったんスクランブルデータをダウンロードした後に外部記憶装置に記憶されているスクランブルデータを予め決められた手順によって自動的に削除するか、全てのスクランブルが復号化された時点で外部記憶装置に展開されたスクランブルデータを削除あるいは書き換えするようにすれば、次に同じデータ本体を起動しようとしてもスクランブルデータをホストコンピュータから再度ダウンロードしなければできないことになる。従って、無断使用を防止することができる。これは、ローダ自体を同様の処理で削除、あるいは書き換えを行うことにより達成してもよい。

【００１２】上記構成に基づいて必要なデータを１つの受信端末装置２で処理する手順を説明すると、先ず通信衛星３あるいはＣＡＴＶネットワーク５を介してサイクリックに伝送されるデータから、希望するデータ本体を読み込む。これは複数の手段によって達成することができるが、たとえばデータ本体がパケットモードで伝送されているとすれば、個々のパケットの先頭にデータ本体を示す識別コードを付加しておき、受信端末装置２からこの識別コードを入力することによって取り込むことができる。識別コードは一覧表としてサイクリックに伝送しておけば、受信端末装置のモニタ画面で確認することは容易である。このようにして、受信端末装置２では必要なデータ本体を記憶装置に取り込むことができるが、スクランブルが施された状態なので単独では実行することができない。続いて、受信端末装置２から公衆回線網４あるいはＣＡＴＶネットワーク５を介してホストコンピュータ１をアクセスし、上記識別コード、あるいはこれと対応するコードを指示してスクランブルデータとローダのダウンロードを要求し、記憶装置内に取り込む。この場合、スクランブルデータとローダを各データ本体ごとに対応したものでなく、汎用のプログラムにしておけば、各データ本体を示す識別コードを入力する必要はない。

【００１３】図３は受信端末装置２がデータ本体、スクランブルデータおよびローダを記憶装置に読み込んだ状態を示す。８はハードディスク装置などの外部記憶装置、９は処理実行のためのメモリ領域であり、既に基本ＯＳが一部の領域を占領している。ここで、外部記憶装置８にはデータ本体、スクランブルデータおよびローダが格納されているが、これらの各データはファイルによって明確に独立した状態である。そして、キーボードやマウスからローダの起動を指示すると、基本ＯＳが外部記憶装置８をアクセスし、メモリ領域９の空領域に対して処理を展開し、図４のメモリ状態が達成される。即ち、空領域にはローダ１０とスクランブルデータ１１が読み込まれ、基本ＯＳからローダ１０に移行された実行権のもとにローダ１０が外部記憶装置８に存在するデータ本体を読み込みながらスクランブルデータを参照してデータ本体を復号する。この場合、外部記憶装置８に格納されているスクランブルデータおよびローダは削除される。削除するタイミングは問わないが、少なくとも受信端末装置２においてデータ処理が終了するまでには完了していなければならない。なお、外部記憶装置８から削除するのは、スクランブルデータあるいはローダの何れか一方だけでもよい。また、これらを外部記憶装置８からメモリ領域９にいったんコピーして、後に削除する過程に代えて、コピーと削除を同時に行う処理、即ち移行によっても目的は達成できる。

【００１４】次に、図５には別の手順を示す。外部記憶装置８からローダを指示して処理を開始すれば、先ずメモリ領域９の空領域にローダ１０とスクランブルデータ１１が読み込まれる。続いてローダ１０がスクランブルデータ１１を参照しながら外部記憶装置８に格納されているデータ本体を読みだし、空領域に展開を進める。そして、少なくともデータ本体の実行ファイルなど、スクランブルが施されているデータの展開を完了する。そして、展開が完了すればスクランブルデータおよびローダを書き換える。このようにすれば、次の実行を希望する場合には再度スクランブルデータおよびローダを取得しなければならず、無断使用を回避することができる。なお、書き換えはスクランブルデータあるいはローダの何れか一方だけでもよい。

【００１５】

【発明の効果】本発明ではデータ容量が大きい部分を伝送効率が高い通信方式とし、無断利用を防止するためのファイルを双方向通信で伝送することとしたので、全体

の伝送効率は飛躍的に向上すると共に、ホストコンピュータにおける情報管理も効率的に行うことができるようになる。また、各受信端末装置においても、いったんスクランブルが施されたデータ本体を復号してしまえば、復号に必要なローダやスクランブルデータが削除されたり、書き換えられることになるので、再度の実行は不可能になり、再びホストコンピュータに対して要求を行わなければならず、無断利用を回避することができる。

【図面の簡単な説明】

【図１】本発明を適用するための通信システムのブロック図、

【図２】同、別の通信システムのブロック図、

【図３】スクランブルの復号手順を示すブロック図、

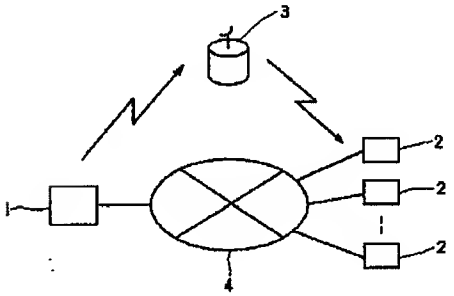
【図４】同、ブロック図、

【図５】同、ブロック図である。

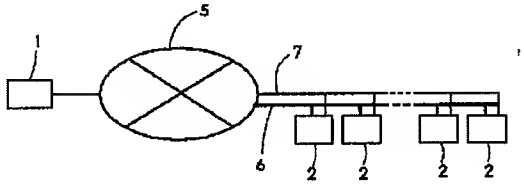
【符号の説明】

1	ホストコンピュータ
2…2	受信端末装置
3	通信衛星
4	公衆回線網
5	ＣＡＴＶネットワーク
6	上りライン
7	下りライン
8	外部記憶装置
9	メモリ領域
１０	ローダ
１１	スクランブルデータ

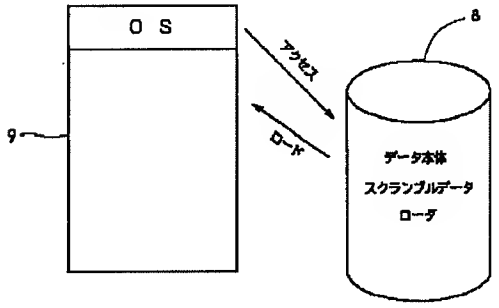
【図１】



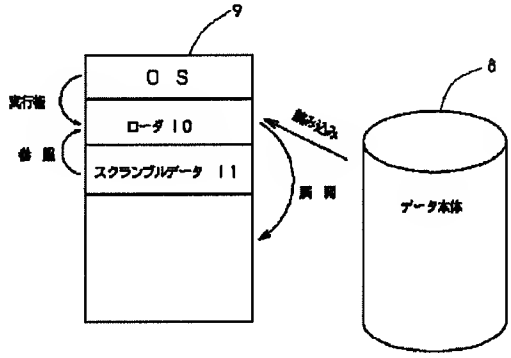
【図２】



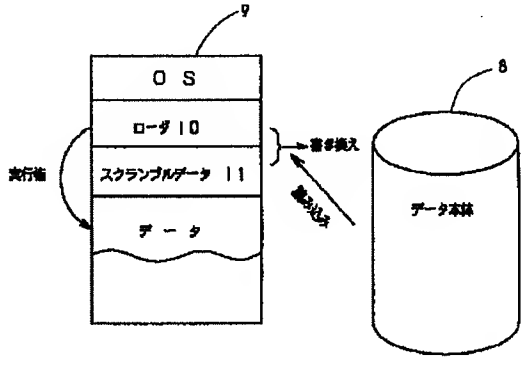
【図３】



【図４】



【図５】



フロントページの続き

(51) Int. Cl.⁶	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｋ　1/00		Ｚ		

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **07-202877**

(43)Date of publication of application : **04.08.1995**

(51)Int.Cl. **H04L 9/00**
H04L 9/10
H04L 9/12
G09C 1/00
H04K 1/00

(21)Application number : **05-353626**

(22)Date of filing : **27.12.1993**

(71)Applicant : **SOFUITSUKU:KK**
TSUYOKA:KK

(72)Inventor : **TSUMURA MIOJI**

(54) DATA SCRAMBLER

(57)Abstract:

PURPOSE: To prevent illegal use of scramble data without permission by down-loading scramble decoding data and a loader from a host computer on individual request from each reception terminal equipment.

CONSTITUTION: The transmission data are made up of data main body applying scrambling to datascramble data and a loaderthe data main body requiring a high transmission capacity are sent via a communication satellite 3 with high transmission efficiencyand the scramble data and the loader are sent via a public line network 4 to a reception terminal equipment 22 respectively from a host computer 1. The reception terminal equipment 22 down-loads the scramble data and the loader to its main storage device or deletes the scramble data when the scrambling is decodedThussame data main body are started nextthe scramble data have to be down-loaded again from the hostcomputerand the use of the data without permission is inhibited.

CLAIMS

[Claim(s)]

[Claim 1]While it is cyclic and a data body to which it became from a host computer and two or more receiving terminal devicesand scramble was given from this host computer by one-way communication to each receiving terminal device is transmittedThe above-mentioned host computer and each receiving terminal device are connected with a two-way communication networkA scramble device of data downloading a loader which performs scramble data which decodes the

above-mentioned scramble from the above-mentioned host computer according to an individual demand from each receiving terminal deviceand a data body.
[Claim 2]In a receiving terminal devicea data bodyscramble dataand a loader are once stored in an external storageA scramble device of the data according to claim 1 in which the above-mentioned loader and scramble data are shifted to vacant regions of a main memory unitand the above-mentioned loader develops a data body with reference to the above-mentioned scramble data.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]This invention relates to the new device for giving scramble to the data transmitted in radio or a wire communication.
[0002]
[Description of the Prior Art]Data transfer technique progresses by leaps and boundsand communication is performed by personal computers at the present using the telephone line and the specific circuit. The digital communication technique by radio is also developedand PCM transmission etc. are prosperous. By the wayit is enough just to write a packet numberan error correcting codeetc. for packet communication in additionfor examplewithout processing it especially into datawhen the data transmitted is gratis release data.
[0003]
[Problem(s) to be Solved by the Invention]Howeverthe frequency where a secret is required depending on the contents of data is also very high now when information value is increasing. Thereforejust before transmitting the data which becomes symmetrical [transmission] from the former by data communicationsscramble is given with an encoderthe decoder for canceling scramble is provided in the receiving setand it is common to transmit according to the protocol on which it decided.
[0004]Howeverin the encoder for giving scramblein order to code data according to a fixed procedureit has an enciphered programbut once it will be decodeddata will be stored in the raw state. Thereforeeven if it pays a utilization charge about the first data usefrom the 2nd timesit can use now without a fee easily and the problem of unapproved use occurs substantially.
[0005]In this inventioneven if it performs once in view of these factsa re-degree aims at providing the device for the encryption which is hard to be decoded easily.
[0006]
[Means for Solving the Problem]In this inventionit consists of a host computer and two or more receiving terminal devices to achieve the above objectsWhile it is cyclic and a data body to which scramble was given from this host computer by one-way communication to each receiving terminal device is transmittedIt was connected with a two-way communication networkand the above-mentioned host

computer and each receiving terminal device adopted a means to download a loader which performs scramble data which decodes the above-mentioned scramble from the above-mentioned host computer according to an individual demand from each receiving terminal deviceand a data body.
[0007]In a receiving terminal devicea data bodyscramble dataand a loader were once stored in an external storagethe above-mentioned loader and scramble data were shifted to vacant regions of a main memory unitand a means by which the above-mentioned loader developed a data body with reference to the above-mentioned scramble data was used.
[0008]
[Function]It is for applying the portion considered that transmitting a data body by one-way communication from a host computer has large data volume to a transmission mode with high transmission efficiency. A means to connect each receiving terminal device with a host computer by two-way communication is because transmission of the file according to the demand from a receiving terminal device is enabled. A means to give scramble to a data body and to transmit to it in multiple address avoids unapproved use of data.
[0009]
[Example]Hereafterone example of this invention is described according to the attached drawing. Firstas a system for data communicationsthe network of drawing 1 or drawing 2 is adopted. Drawing 1 is the network for which satellite communication and a public network were usedandas for the host computer by the side of data supplyand 2--2a communications satellite and 4 are public networkssuch as a digital channela receiving terminal device and 3 1respectively. From the host computer 1information is transmitted by one-way communication to the receiving terminal device 2and two-way communication is performed by the public network 4. Drawing 2 is connected in CATV network 5 where the host computer 1 and the receiving terminal device 2--2 used optical communications etc. using the CATV network. CATV network 5 adopted by this example makes two-way communication possiblean uphill line and 7 get down and 6 is a line. Howeverwhen using the CATV network which has the existing one-way communication functionit is also free that a public network substitutes the going-up line 6.
[0010]Nextas a data structure which is the target of transmissionit is constituted from this invention by a data bodyscramble dataand the loader. And many data bodies are cyclically transmitted from the host computer 1 to the receiving terminal device 2 via the communications satellite 3 or CATV network 5and scramble data and a loader are individually transmitted via the public network 4 according to the demand of each receiving terminal. Or it is transmitted after processing adding an individual identification signal by another channel with a data body in the case of CATV network 5 etc. Thusdividing data into two kinds of transmission routessince what has huge data volume existsa data body fits communicate mode with high transmission efficiency.
It is because it is necessary to specify the receiving terminal device which is a

request destination by a relation with rate collection on the other hand although the data volume of scramble data or a loaderetc. is small.

[0011]The data body which is the target of transmission is a thing in the state where scramble was givenand scramble data is constituted by a compression dictionarya passwordetc. as the parameter of scrambleand a kind of scramble. A data body here means the data having contained the executable fileand refers to what can be started with a data body independent by a fixed command. A loader is developed to external storages with which the receiving terminal was equippedsuch as an empty memory area of a main memory unitand a hard diskdecoding [are used in order to start a data bodyand] a data body based on scramble data. And an execution right is shifted to the decoded data body. At this timescramble data is also developed by a main memory unit or the external storage with a loader. Therefore. [whether the scramble data memorized by the external storage once downloading scramble data to a main memory unit is automatically deleted by the procedure which was able to be decided beforehandand] It cannot doif the scramble data developed by the external storage is deleted or rewritten when all the scramble is decryptedand scramble data is not again downloaded from a host computer even if it is going to start the same data body as the next. Thereforeunapproved use can be prevented. This may attain the loader itself by performing deletion or rewriting by the same processing.
[0012]Explanation of the procedure of processing required data with the one receiving terminal device 2 based on the above-mentioned composition will read the data body to wish to have from the data first transmitted cyclically via the communications satellite 3 or CATV network 5. Although two or more means can attain thisif the data body is transmitted by the packet modefor exampleit can incorporate by adding the identification code which shows a data body to the head of each packetand inputting this identification code from the receiving terminal device 2. An identification code is easy to check in the monitor display of a receiving terminal deviceif it transmits cyclically as a table. Thusalthough a required data body can be incorporated into memory storage in the receiving terminal device 2since it is in the state where scramble was givenif independentit cannot perform. Thenthe host computer 1 is accessed via the public network 4 or CATV network 5 from the receiving terminal device 2it points to the above-mentioned identification codeor this and a corresponding codedownload of scramble data and a loader is requiredand it incorporates in memory storage. In this caseif it is not the thing corresponding for every data body and scramble data and a loader are made the general-purpose programit is not necessary to input the identification code which shows each data body.
[0013]Drawing 3 shows the state where the receiving terminal device 2 read a data bodyscramble dataand a loader into memory storage. 8 is external storagessuch as a hard disk drive9 is a memory area for processing executionand the fundamental OS already occupies some fields. Herealthough a data bodyscramble dataand a loader are stored in the external storage 8each of these

data is in the state which became independent clearly by a file. And if starting of a loader is directed from a keyboard or a mousea fundamental OS will access the external storage 8processing will be developed to the vacant regions of the memory area 9and the memory state of drawing 4 will be attained. That iswhile the loader 10 and the scramble data 11 are read into vacant regions and the loader 10 reads the data body which exists in the external storage 8 into the basis of the execution right which shifted to the loader 10 from a fundamental OSa data body is decoded with reference to scramble data. In this casethe scramble data and the loader which are stored in the external storage 8 are deleted. Although the timing to delete does not askby the time data processing is completed in the receiving terminal device 2 at leastit must be completed. As for deleting from the external storage 8either one of scramble data or a loader is. It replaces with the process in which once copy these to the memory area 9and they are behind deleted from the external storage 8and the purpose can be attained by the processing which performs copy and deletion simultaneouslyi.e.shift.

[0014]Nextanother procedure is shown in drawing 5. If it points to a loader from the external storage 8 and processing is startedthe loader 10 and the scramble data 11 will be first read into the vacant regions of the memory area 9. Thenwhile the loader 10 refers to the scramble data 11the data body stored in the external storage 8 is readand deployment is advanced to vacant regions. And the executable file of a data bodyetc. complete at least deployment of the data in which scramble is given. And if deployment is completedscramble data and a loader will be rewritten. If it does in this waywhen you wish the next executionscramble data and a loader must be acquired againand unapproved use can be avoided. As for rewritingeither one of scramble data or a loader is.

[0015]

[Effect of the Invention]In this inventiondata volume makes a large portion a communication method with high transmission efficiencyand since it presupposed that the file for preventing unapproved use is transmitted by two-way communicationthe whole transmission efficiency can improve by leaps and boundsand it can also perform information management in a host computer efficiently. Since a loader required for decoding and scramble data will be deleted or it will be rewritten if the data body in which scramble was once given is decoded also in each receiving terminal deviceThe execution for the second time can become impossiblemust require from a host computer againand can avoid unapproved use.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The block diagram of the communications system for applying this invention

[Drawing 2]**** -- the block diagram of another communications system

[Drawing 3]The block diagram showing the decoding procedure of scramble
[Drawing 4]**** block diagram
[Drawing 5]It is a **** block diagram.
[Description of Notations]
1 Host computer
2 --2 Receiving terminal device
3 Communications satellite
4 Public network
5 CATV network
6 An uphill line
7 Get down and it is a line.
8 External storage
9 Memory area
10 Loader
11 Scramble data